A Note on Random Number Generator of Chung et. al.

by

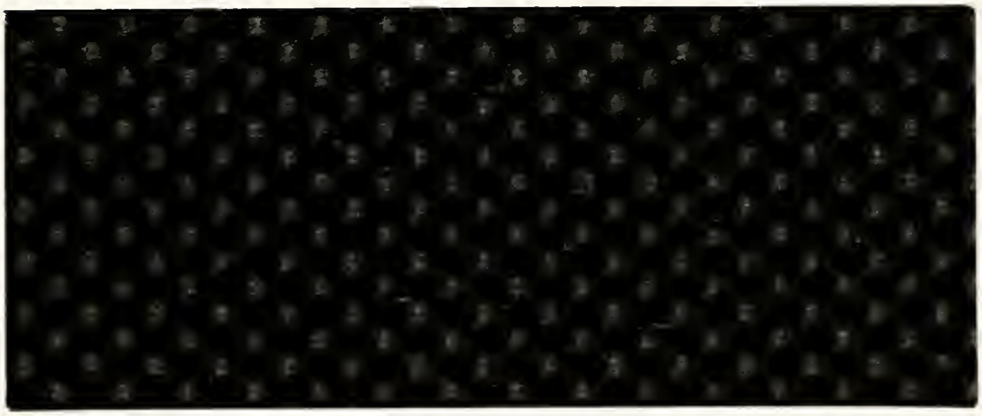
Ora E. Percus[†]

Ultracomputer Note #113
December, 1986

Ultracomputer Research Laboratory

New York University
Courant Institute of Mathematical Sciences
Division of Computer Science
251 Mercer Street, New York, NY 10012

NYU UCN-113 c.1
Percus, Ora E
A note on random number
generator of Chung et al.



A Note on Random Number Generator of Chung et. al.

by

Ora E. Percus†

Ultracomputer Note #113
December, 1986

This work was supported by the Applied Mathematical Sciences Program of the US Department of Energy under contract DE-AC02-76ER03077.

ABSTRACT

We derive the probability distribution $P\{X_n=x\}$ for a random walk satisfying $X_0=0$; $P\{X_{n+1} = (2X_n+1)\ mod\ p\} = P\{X_{n+1} = (2X_n-1)\ mod\ p\} = \frac{1}{2}$ for $n \geq 0$ and p odd integer.

Chung et. al. [1] present a scheme for combining, or shuffling, random number generators of the form

$$X_{n+1} \equiv aX_n + b(mod\ p), \quad p\ odd; \quad X_0 \equiv 0.$$

Their scheme consists of choosing b from another truly random generator, in particular they deal with the following three cases:

$$\text{I:} \quad a = 1, \quad b = 0, 1, -1 \quad \text{each} \quad \text{w.p. } \frac{1}{3}$$

$$\text{II:} \quad a = 2, \quad b = 0, 1, -1 \quad \text{each} \quad \text{w.p. } \frac{1}{3}$$

$$\text{III:} \quad a = 2, \quad b = 1, -1 \quad \text{each} \quad \text{w.p. } \frac{1}{2}$$

In each case, they furnish the number of steps which suffice to guarantee randomness, after obtaining the variation distance (see (1.6)) as a measure of closeness to uniformity.

The purpose of this note is to give a simple derivation of the distribution

$$P\{X_n = x\} \quad x = 0,\ldots,p-1$$

for case III, from which the proof of Theorem 5 in [1] is easily obtained.

Theorem:

Let $X_0, X_1, X_2, \ldots$ be a sequence of random variables satisfying

$$X_0 \equiv 0.$$

(1.1)

$$P\ \{X_{n+1} = 2X_n+1\ mod\ p\} = P\{X_{n+1} = 2X_n-1\ mod\ p\} = \frac{1}{2}$$

for $n \geq 0$ and p odd integer.

Let

$$2^n = \alpha p + \beta + 1 \quad 0 \leq \beta < p-1$$

Then for $x = 0,\dots, p-1$

$$P\{X_n = x\} = \begin{cases} \dfrac{\alpha+1}{2^n} & \text{if } x=(\beta-2j)\ mod\ p \qquad j=0,\dots,\beta \\ \dfrac{\alpha}{2^n} & otherwise. \end{cases}$$

Proof:

For $n \geq 1$ define

(1.2)

$$X_n = 2^{n-1}\sigma_1 + 2^{n-2}\sigma_2 + \dots + \sigma_n \ \ mod\ p$$

where σ_i, $i=1,\dots,n$ are i.i.d and

$$P\{\sigma_i = +1\} = P\{\sigma_i = -1\} = \frac{1}{2}\ .$$

Then, the sequence (1.2) satisfies (1.1) and

(1.3)

$$E\left\{e^{ik\frac{2\pi}{p}X_n}\right\} = \prod_{l=0}^{n-1} E\left\{e^{ik\frac{2\pi}{p}2^l\sigma_{n-l}}\right\} = \prod_{l=0}^{n-1}\left\{\frac{1}{2}e^{ik\frac{2\pi}{p}2^l} + \frac{1}{2}e^{-ik\frac{2\pi}{p}2^l}\right\}$$

$$= \prod_{l=0}^{n-1}\cos k\,\frac{2\pi}{p}2^l = \begin{cases} \dfrac{\sin 2^n\, 2\pi k/p}{2^n \sin\, 2\pi k/p} & if\ \ k \neq 0 \\ 1 & if\ \ k = 0 \end{cases}$$

But

$$P\{X_n = x\} = \frac{1}{p}\sum_{k=0}^{p-1} e^{-ik\frac{2\pi}{p}x}\, E\left\{e^{ik\frac{2\pi}{p}X_n}\right\}$$

(1.4)

$$= \frac{1}{p}\left\{1 + \sum_{k=1}^{p-1} e^{-ik\frac{2\pi}{p}x}\, E\left\{e^{ik\frac{2\pi}{p}X_n}\right\}\right\}.$$

For $2^n = \alpha p+\beta+1 \quad 0\le\beta<p-1 \quad \sin 2^n \,\frac{2\pi k}{p} = \sin(\beta+1)\frac{2\pi k}{p}$ hence, using (1.3) and (1.4) we obtain

$$P\{X_n = x\} = \frac{1}{p}\left\{1+\frac{1}{2^n}\sum_{k=1}^{p-1} e^{-ik\frac{2\pi}{p}x}\,\frac{\sin(\beta+1)\frac{2\pi k}{p}}{\sin\frac{2\pi k}{p}}\right\}$$

$$=\frac{1}{2^n p}\left\{2^n-(\beta+1)+\sum_{k=0}^{p-1} e^{-ik\frac{2\pi x}{p}}\,\frac{\sin(\beta+1)\frac{2\pi k}{p}}{\sin\frac{2\pi k}{p}}\right\}$$

$$=\frac{1}{2^n p}\left\{\alpha p+\sum_{j=0}^{\beta}\sum_{k=0}^{p-1} e^{\frac{2\pi i k}{p}(\beta-2j-x)}\right\}$$

or

$$P\{X_n = x\} = \frac{1}{2^n p}\left\{\alpha p+\sum_{j=0}^{\beta} p\,\delta_{x,\beta-2j\,\equiv\,0 \; mod\; p}\right\}$$

(1.5)

$$=\begin{cases}\dfrac{\alpha+1}{2^n} & \text{if } x=(\beta-2j)\ mod\ p \qquad j=0,\ldots,\beta\\[2ex] \dfrac{\alpha}{2^n} & otherwise.\end{cases}$$

for $x=0,\ldots,p-1$. Q.E.D.

The variation distance is defined in [1] as

(1.6)

$$\frac{1}{2}\sum_{x=0}^{p-1}\left|P\{X_n=x\}-\frac{1}{p}\right|,$$

since $\frac{\alpha}{2^n} < \frac{1}{p} < \frac{\alpha+1}{2^n}$ an immediate consequence of (1.5) is

$$\frac{1}{2}\sum_{x=0}^{p-1}\left|P\{X_n=x\}-\frac{1}{p}\right| = \frac{(\beta+1)[p-(\beta+1)]}{2^n p}$$

which is Theorem 5 in [1].

1. Acknowledgement

I would like to thank Malvin Kalos for introducing me to the problem that motivated this work.

2. References

[1] Chung, F.R.K., P. Diaconis and R.L. Graham. "Random Walks Arising in Random Number Generation", Annals of Probability.

NYU UCN-113 c.1
Percus, Ora E
A note on random number generator of Chung et al.

NYU UCN-113 c.1
Percus, Ora E
A note on random number generator of Chung et al.

This book may be kept JUN. 01 1987
FOURTEEN DAYS
A fine will be charged for each day the book is kept overtime.

GAYLORD 142 PRINTED IN U.S.A.